Minneapolis
City of Lakes

External Penetration Assessment and Database Access Review

Performed by Protiviti, Inc.
At the request of Internal Audit
April 25, 2012

Agenda

1. Introductions
2. Assessment/Review Area
   - a. External Penetration Assessment
   - b. Database Access Review
3. Questions

Agenda For Each Area
▪ Overview, Technology Background & Risks
▪ Approach
▪ Positive Observations/Observed Vulnerabilities

Protiviti Overview

Protiviti is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. We have more than 2500 employees in 70 offices that have served more than 35 percent of FORTUNE® 1000 and Global 500 companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half International Inc. (NYSE: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

Internal Audit & Financial Controls

- Audit Committee Advisory
- Information Technology (IT) Audit Services
- Internal Audit Co-Sourcing
- Internal Audit Full Outsourcing
- Internal Audit Quality Assurance Reviews
- Internal Audit Technology & Tool Implementation
- Internal Audit Transformation
- Start-up & Development Advice
- High Value Auditing
- Data Mining & Analytics
- Financial Controls & Sarbanes-Oxley Compliance
- J-SOX Compliance

Transaction Services

- Merger and Acquisition Services
- Public Company Transformation

Finance & Accounting Excellence

- Performance & Information Management
- Finance Process Optimization
- Financial Reporting Remediation & Compliance
- International Financial Reporting Standards (IFRS)
- Financial Controls & Sarbanes-Oxley Compliance
- Enterprise Risk Management

Litigation, Restructuring & Investigative Services

- Corporate Restructuring & Recovery
- E-Discovery
- Financial Investigations
- Fraud Risk Management
- Litigation Consulting

Business Operations Improvement

- Supply Chain
- Capital Projects & Contracts
- Loss Prevention
- Revenue Risks
- AP Recovery Services

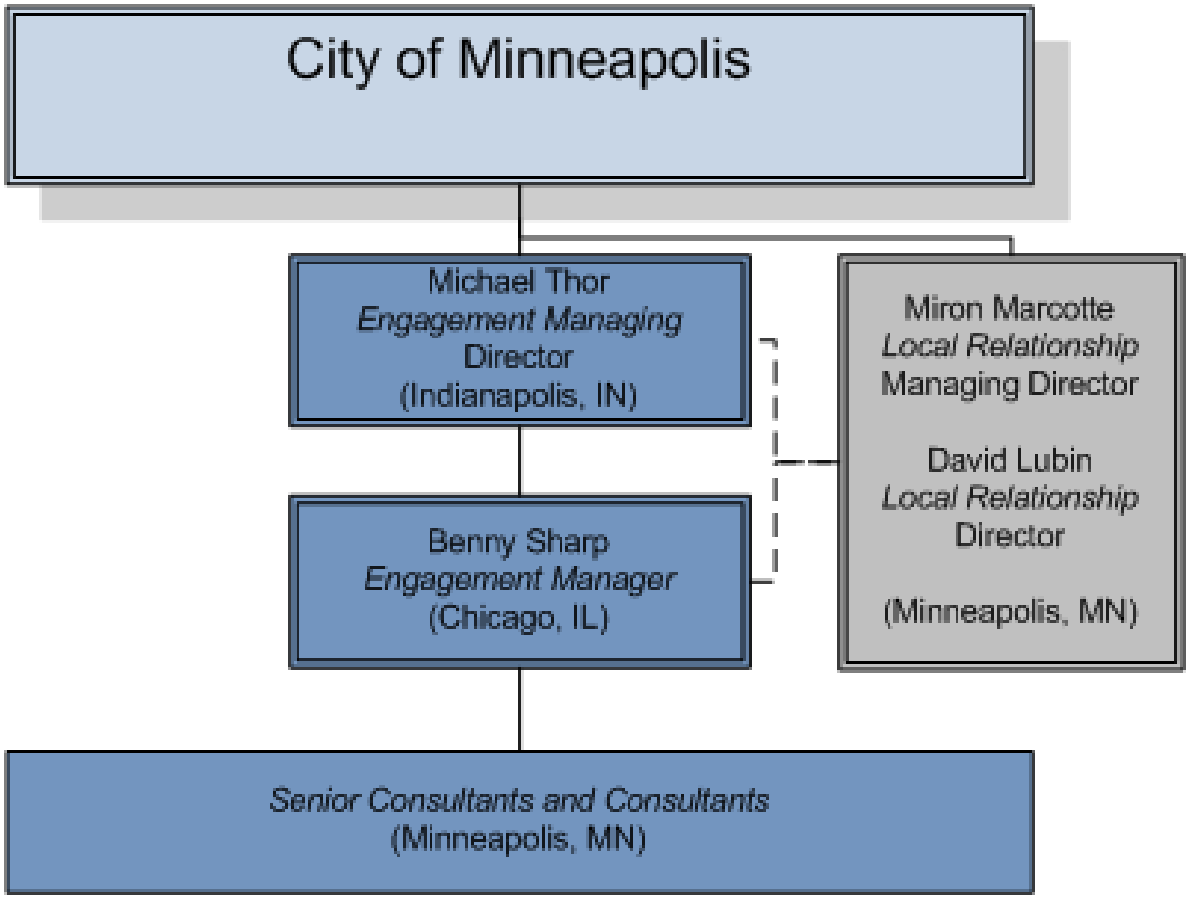
Risk & Compliance

- Risk Strategy & Management
- Compliance

Information Technology Consulting

- Managing the Business of IT
- Managing Applications & Data
- Managing IT Security & Privacy

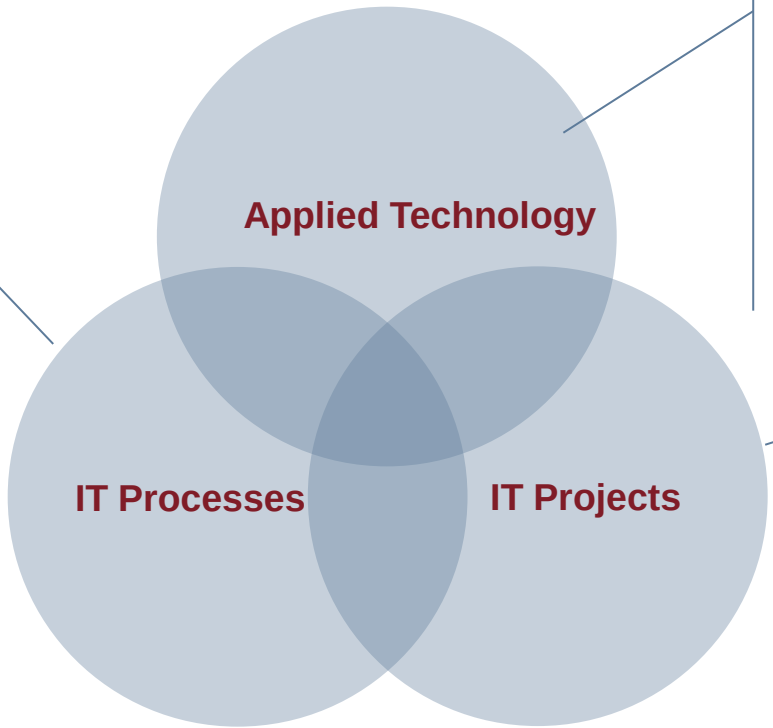
Protiviti Team



IT Audit Universe

The IT audit universe is made up of applied technology (applications, supporting infrastructure), IT processes, and significant IT projects/initiatives.

- Applications (i.e.; PeopleSoft)
- Databases (i.e.; Oracle)
- Operating Systems (i.e.; Microsoft Windows)
- Infrastructure Components (i.e.; Servers, Firewalls)



- Processes that enable IT to deliver service to its end users based on existing frameworks like COBIT, ITIL, ISO. For example:
  - Change Management
  - Disaster Recovery
  - IT Shared Services
  - Manage IT Assets
  - Manage Infrastructure
  - PMO
  - Manage Security
  - Vendor Management

Any in-process or planned IT project (including new applications, changes to IT processes, data center moves, other strategic initiatives, etc.)

Rating Definitions

Risk Level	Significance
High	Observed vulnerabilities assigned a high risk level are considered to present an imminent and significant threat and should be addressed as soon as possible.
Medium	Observed vulnerabilities assigned a medium risk level do not pose an immediate threat, but could likely cause a noticeable impact. These should be addressed in a timely manner once high level risks have been addressed.
Low	Observed vulnerabilities assigned low risk level are considered to present threats that are unlikely to occur and would have a smaller impact. These should receive the lowest priority when being addressed.

These observed vulnerabilities are assigned a subjective rating and provide management with information about the condition of risks and internal controls at a point in time. Future changes in environmental factors and actions by personnel may adversely impact or enhance these risks and controls in ways that this assessment did not and cannot anticipate.

External Penetration Assessment

Overview

Attempted to find commonly known vulnerabilities that a person outside of the organization with malicious intent ("attacker") would try to exploit against the City of Minneapolis' network.

Example

External threat example

- The hacking group “Anonymous” recently made the news by attacking several government and corporate systems in an attempt to steal data and strong-arm organizations.
  - Obtained and publicly released user information, credit card data and other private data

What are attackers after?

- Private Data (Credit Card Numbers, Social Security Numbers, Financial Data)
- Control of Organizations
- Money: proprietary and private data is valuable

Risks

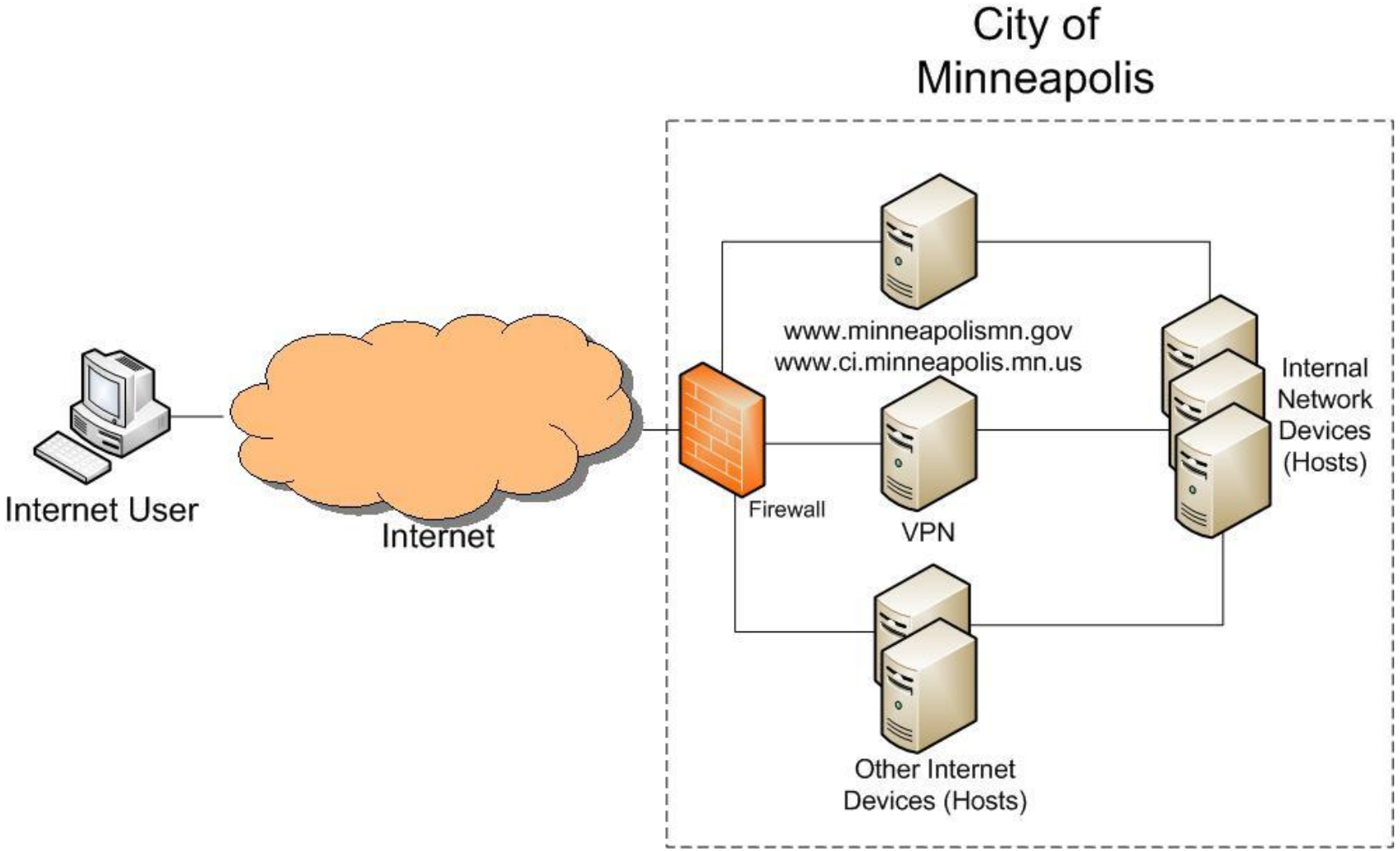
Risks

- Unauthorized access to data classified as “not public” and internal systems
- Loss of availability of services relied upon by people and organizations
- Modification of data including falsifying records and defacement of public facing websites and services

Implications

- Loss of user trust and harm to the City’s brand and image
- Financial loss and responsibility to clean up and repair any internal and external damages

Overview


City of Minneapolis
www.minneapolismn.gov
www.ci.minneapolis.mn.us
Internal Network Devices (Hosts)
Internet User
Internet
Firewall
VPN
Other Internet Devices (Hosts)

Assessment Approach

Objective
Assess the external security posture of the network and users

External Network Approach
1. Discovered external hosts
2. Scanned and tested for common vulnerabilities
3. Attempted to exploit vulnerabilities with a focus on obtaining unauthorized access

Social Engineering Approach
1. Selected a sample of 20 employees to call
2. Called employees and attempt to gain information deemed “not public” such as passwords

Positive Observations

Several positive attributes of the control environment were observed.

Positive Observations
1. Unauthorized access to systems or services was not obtained.
2. Default and/or weak passwords were not found.
3. Firewalls prevented access to internal networks.
4. Unnecessary services were not listening on the internet.

Observed Vulnerabilities

	Observed Vulnerability	Criticality	Expected Completion Date
1	Security Awareness	Medium	12/31/2013
2	Missing updates and patches	Medium	12/31/2012
3	Improper Output Sanitization	Medium	12/31/2012
4	External FTP (File Transfer Protocol)	Medium	12/31/2012
5	Web Platform Configuration	Low	12/31/2012
6	Insecure SSL (Secure Sockets Layer) Configuration	Low	12/31/2013

Database Access Review

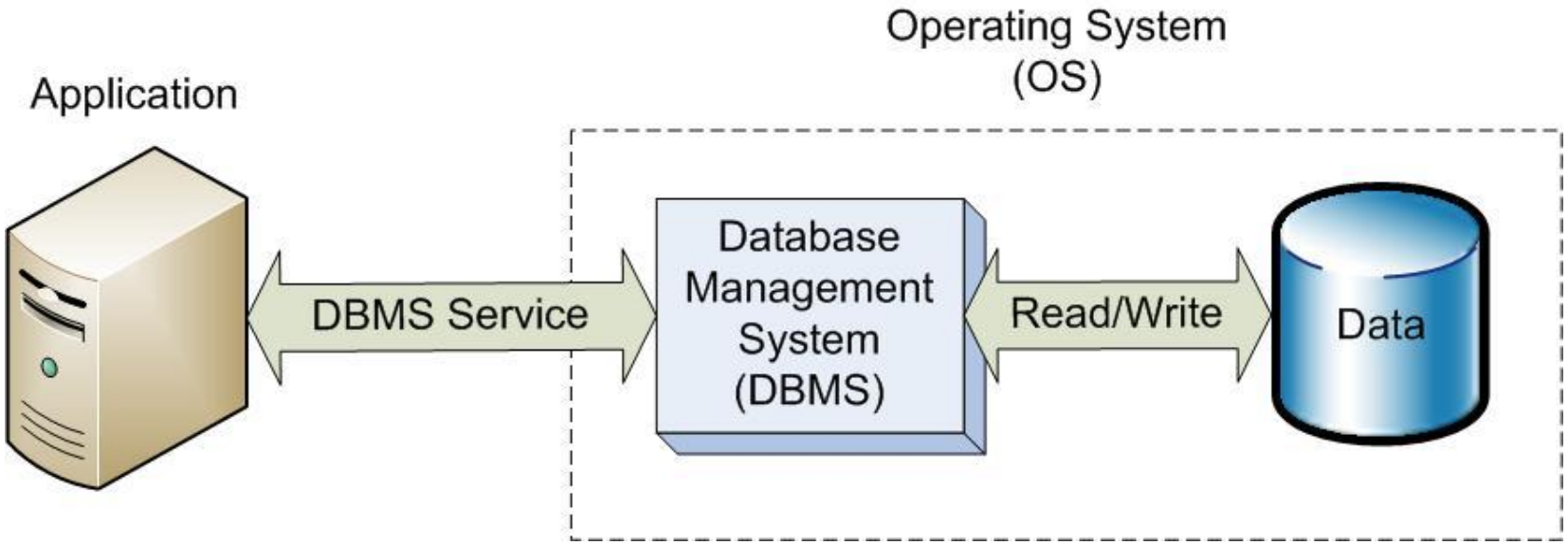
Overview

Reviewed the controls in place for access to data used by Oracle PeopleSoft systems to identify any potential for inappropriate access to systems and data.

PeopleSoft

PeopleSoft is an Enterprise Resource Planning (ERP) application made by Oracle which can manage information for many different parts of an organization.

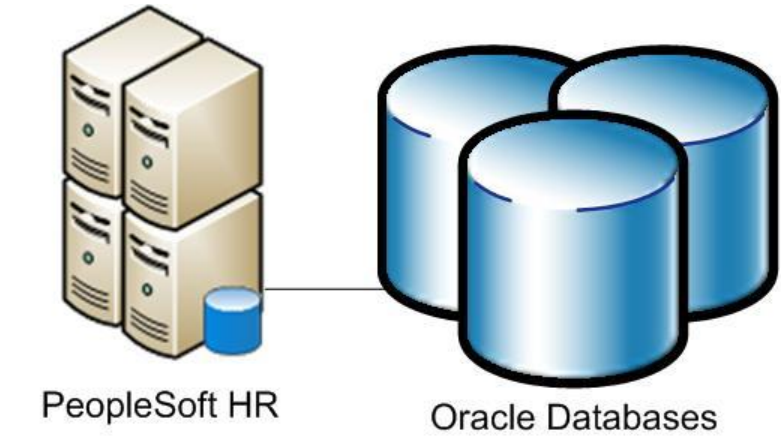
Overview

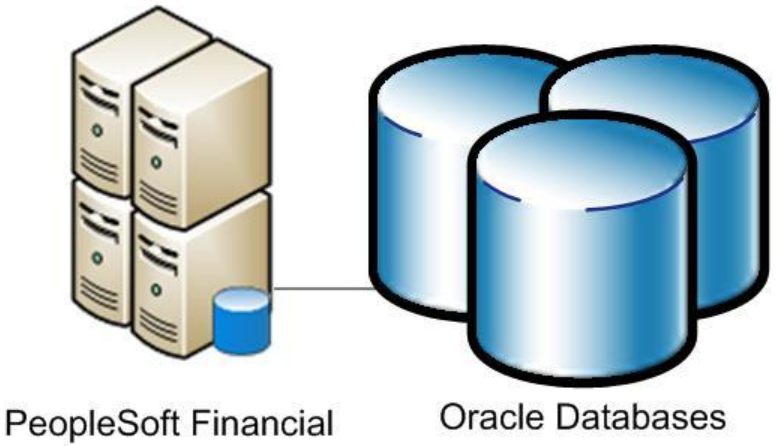


- Applications use databases to access, organize and store data.
- A Database Management System (**DBMS**) is used to actually manage the data and communicate with the application.
- The DBMS is installed on an Operating System (**OS**, such as Microsoft Windows).
- Both the OS and DBMS have users and access control configurations.

Oracle PeopleSoft Overview

- Examples of “not public” data stored in these databases;
  - Employee Data
  - Citizen Data
  - Payroll Data
  - Financial Data
- 5 different environments;
  - Production
  - Production-DR (Disaster Recovery)
  - QA (Quality Assurance)
  - Development
  - Training/QA
- PeopleSoft uses Oracle DBMS.
- The Oracle PeopleSoft DBMS is installed on Microsoft Windows as the OS.





Risks

Risks

- Unauthorized access to view or modify data
  - Employees (Active and Terminated)
  - Third-Party Vendors or Contractors
  - Shared Accounts (Single account for multiple users)
- Inappropriate access for authorized users
  - Access to data classified as “not public” which is beyond the scope of job role
  - Extraneous administrative privileges

Implications

- Exposure of data classified as “not public” such as employee personal information or financial data
- Tampering with or modification of data
- Modification of systems including loss of availability

Approach

The following items were reviewed for both the OS and DBMS associated with each PeopleSoft implementation:

- Reviewed how authentication and access controls are implemented and restrict access
- Reviewed the account management process including user approval, creation, maintenance, tracking, and removal
- Verified that an account review process has been properly implemented
- Reviewed current user and administrator account access rights for appropriateness

Positive Observations

Several positive attributes of the control environment were observed.

Positive Observations
1. Privileges assigned to users were appropriate for the associated job functions.
2. Secure authentication mechanisms were in place.
3. Logging and monitoring of access related events were being performed.

Observed Vulnerabilities

	Observed Vulnerabilities	Criticality	Expected Completion Date
1	Incomplete Policy and Procedure Documentation	Medium	12/31/2012
2	Lack of Formalized Account Management Process	Medium	12/31/2012
3	Shared and Unknown Database Accounts	Medium	12/31/2012

Minneapolis
City of Lakes

Questions?